TrustIoT Framework for Industry 4.0

"API Security: Authentication, rate limiting & access controls"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *TrustIoT Framework for Industry 4.0* |
| Version: | *1* |
| Document Author: | *Jibran Saleem* |
| Document Owner: |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc176333451)

[2. Purpose 4](#_Toc176333452)

[3. Scope 4](#_Toc176333453)

[4. Policy Statement 4](#_Toc176333454)

[4.1. Authentication 4](#_Toc176333455)

[4.2. Rate Limiting and Throttling 4](#_Toc176333456)

[4.3. Access Controls 4](#_Toc176333457)

[5. Responsibilities 5](#_Toc176333458)

[6. Breaches of Policy 5](#_Toc176333459)

[7. Document Management 5](#_Toc176333460)

# Introduction

Application Programming Interfaces (APIs) are fundamental to the functioning of the Internet of Things (IoT) ecosystem, enabling communication and data exchange between various devices, services, and applications. However, the open nature of APIs can expose them to unauthorised access, misuse, and exploitation. This policy establishes a framework for ensuring the security of IoT APIs through robust authentication, rate limiting, and access control mechanisms.

# Purpose

The purpose of this policy is to define the policies and procedures for securing APIs within the organisation's IoT infrastructure. This policy aims to:

* Protect APIs from unauthorised access and misuse.
* Safeguard the confidentiality, integrity, and availability of data exchanged through APIs.
* Prevent denial-of-service (DoS) attacks and other forms of API abuse.
* Ensure compliance with industry best practices and regulatory requirements.

# Scope

This policy applies to all APIs exposed by IoT devices, systems, and applications within the organisation's network, regardless of whether they are internal or external facing.

# Policy Statement

## Authentication

* **API Keys:** Unique API keys shall be issued to authorised users and applications to authenticate their access to APIs.
* **Strong Authentication:** Where appropriate, stronger authentication mechanisms, such as OAuth 2.0 or OpenID Connect, shall be implemented to provide enhanced security.
* **Key Management:** API keys shall be securely generated, stored, and managed, with periodic rotation to minimise the risk of compromise.
* **Revocation:** Procedures shall be in place to promptly revoke API keys in case of suspected compromise or when access is no longer required.

## Rate Limiting and Throttling

* **Rate Limits:** Rate limits shall be enforced on API calls to prevent abuse, denial-of-service (DoS) attacks, and excessive resource consumption.
* **Throttling:** Dynamic throttling mechanisms may be implemented to adjust rate limits based on real-time traffic patterns and system load.
* **User Notification:** Users and applications shall be notified when they approach or exceed their allocated rate limits.

## Access Controls

* **Role-Based Access Control (RBAC):** RBAC shall be implemented to restrict API access based on user roles and responsibilities.
* **Granular Permissions:** Fine-grained access control mechanisms shall be employed to allow or deny access to specific API endpoints or data based on user permissions.
* **API Gateway:** An API gateway may be utilised to centralise access control, authentication, and rate limiting for multiple APIs.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **API Developers:** Responsible for designing and implementing APIs with appropriate security controls, including authentication, authorisation, and input validation.
* **IT Department:** Responsible for managing API gateways, access control mechanisms, and monitoring API activity.
* **API Consumers:** Responsible for using APIs responsibly and in compliance with this policy.

# Breaches of Policy

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships.

# Document Management

This document is valid as of [dd/mm/yyyy].

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

* Compliant with the Internet of Things (IoT) Security Framework for Industry 4.0.
* Legislative requirements defined by law, where appropriate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name 1]

Manager